

From Yearly Audits to Continuous Compliance

A year-round security program for PCI readiness

Discussion Focus

Building a foundation for an agile program to avoid the yearly assessment scrambles and surprises

Mindy Milliet

Cyber Advisory Partner &
Global PCI Practice Leader

Frazier & Deeter Advisory, LLC.



Seth Hinson

Cyber Advisory Manager

Frazier & Deeter Advisory, LLC.



John Deason

Cyber Advisory Senior

Frazier & Deeter Advisory, LLC.



Session Opening: Why This Conversation Matters

Point-in-time compliance

Prepare for the audit, gather evidence, respond to findings, and move on.

Continuous compliance

Build security, monitoring, and evidence collection into everyday operations.

PCI DSS is a point-in-time assessment, but the standard expects a continuous program.

Point-in-Time Compliance Falls Short

The relief of ‘making it through another year’ can lead to a false sense of readiness for the next assessment.



Common Challenges Between Assessments

01 **Control ownership gaps/drift**

People and roles can change through the year, this can generate gaps in ownership.

02 **Time-limited manual evidence collection**

Teams scramble to collect evidence when audit season arrives

03 **Changing environments**

Systems, processes, and dependencies change between testing cycles.

04 **Human errors**

People are the core of processes, mistakes can happen.

05 **Limited visibility**

Small issues pile up throughout the year and aren’t visible until the assessor compiles them



Control drift happens between audit moments.

The foundations of a strong program

PCI DSS already has many continuous requirements (scans, scope reviews, etc.), but 12.4.2 and 12.4.2.1 give us a starting point for a continuous program



Year-Round Security Activities

01 **Control monitoring and lookback**

Know whether core controls remain effective. Identify gaps and remediate throughout the year.

02 **Automated/proactive evidence collection**

Work with control owners during downtime to automate their manual collection

03 **Real-time vulnerability tracking**

Build strong accountability and ensure vulnerabilities don’t slip through the cracks

04 **Regular access reviews**

Regular, smaller reviews are less ‘painful’ and more accurate.

05 **Policy and procedure updates**

Keep documentation aligned to reality.

06 **Clear control ownership**

Make accountability visible and measurable.

The goal is clear: smaller, more frequent checkpoints and self-assessments reduce risk and workload when the assessment comes.

Scope ownership and maintenance

The heart of a strong continuous program is a well documented and maintained scope, which should be updated continuously as your organization grows and changes.



Scope Book Example #1

Account Data flow and storage: the core of PCI scope

Description of Account Data Flows

Identify in which of the following account data flows the assessed entity participates.

Authorization	Capture	Settlement	Chargeback/Dispute	Refunds	Other:	Responsible Team / PoC

Identify and describe all data flows.

Descriptions should include how and where account data enters the environment, is transmitted, is processed, is stored, and how and why any personnel access the account data. Add rows as necessary.

Account Data Flow / Payment Stage	Account Data Elements Involved (e.g., PAN, expiry, cardholder name, SAD prior to authorization)	Source / Origin	Destination	Systems / Applications Involved	Network / Zone	How Account Data Is Received / Transmitted and Business Purpose	Protection in Transit (e.g., HTTPS/TLS, SFTP, private network)	Storage Location(s), if Any	Diagram Reference / Version	Responsible Team / PoC

Storage of account data

Identify all databases, tables, and files storing account data and provide the following details:

Data Store (i.e., database, file server, repository)	File / Table / Field Names	Account Data Elements Stored (e.g., PAN, expiry, cardholder name, SAD prior to authorization)	How Data Is Secured (encryption, hashing, tokenization, truncation, etc.)	How Access to Data Stores Is Logged	Backup / Replica / Geographic Locations	Retention Period and Business Justification	Retention Enforcement Mechanism (automatic/manual purge and frequency)	Quarterly Retention / Deletion Validation (method and evidence reference)	Data Discovery Method / Last Performed	Responsible Team / PoC

Scope Book Example #2

Diagrams and segmentation

Network & Account Data Flow Diagram Inventory

Maintain a simple inventory of the diagrams used to support PCI DSS scope. Update diagram references when significant changes occur and during periodic scope validation.

Diagram Name / Reference	Diagram Type (Network / Account Data Flow)	Scope / Environment Covered	Owner	Version / Date	Last Reviewed / Updated	Notes / Evidence Location

Segmentation Control Inventory

Where segmentation is used to reduce PCI DSS scope, identify the specific enforcement points and the environments separated by each control. Add rows as necessary.

CDE / In-Scope Zone	Segmented / Out-of-Scope Zone	Segmentation Control / Enforcement Point	Technology / Configuration Basis	Permitted Connections / Business Justification	Last Segmentation Test / Evidence Reference	**Responsible Team / PoC**

Scope Book Example #3

Systems and Applications

In-Scope Component Types Identify all types of system components in scope. One row may represent a homogeneous population where the components have the same role, vendor/product/version, scope classification, and environment. Use the Inventory / Asset Group Reference to tie the row to the authoritative inventory or CMDB.										
Type of System Component	Total Number of System Components	Vendor	Product Name and Version	Role / Function Description	Scope Classification (CDE / Connected-to / Security-Impacting)	Environment (Prod / Dev / Test / Corp, etc.)	Network / Segment	Hosting Location / Cloud Account	Inventory / Asset Group Reference	**Responsible Team / PoC**

In-Scope Application										
Application Name	SME / Application Owner	Off-the-Shelf, In-House, or Bespoke? If bespoke, identify developer/team.	Stores / Processes / Transmits Account Data (select all that apply)	Account Data Elements	Displays PAN? (Y/N) If yes, provide masking format.	Hosting Model / Location (on-prem, cloud account, SaaS, etc.)	Payment Function / Role	Code Repository / Development Team (if custom software)	Description	**Responsible Team / PoC**

For more information, contact:

Mindy Milliet - mindy.milliet@frazierdeeter.com

Seth Hinson - seth.hinson@frazierdeeter.com

John Deason - john.deason@frazierdeeter.com

